Form PTO-1449 (MODIFIED)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. 068398-0104	SERIAL NO. 09/818,606
		APPLICANT Virgil D. Gligor et al.	
		FILING DATE March 28, 2001	GROUP ART UNIT 2131

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
MGP	A1	5,757,913	5/26/98	Bellare et al.	380	23	

FOREIGN PATENT DOCUMENTS

	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

MGP	A2	Virgil D. Gligor et al., "Object Migration and Authentication.", IEEE Transactions on software Engineering, vol. SE-5, No. 6, November 1979, pp. 607-611
	A3	Alfred J. MENEZES et al., ""Handbook of Applied Cryptography", pp. 321-367, (1965)
	A4	J. Black et al., "UMAC: Fast and Secure Message Authentication.", Advances in Cryptology-CRYPTO '99, pp. 216-233
	A5	Mihir BELLARE et al., "Keying Hash Functions For Message Authentication", Springer-Verlag Berlin Heidelberg, pp. 216-233, (1996)
	A6	Mihir BELLARE et al., "The Security of Cipher Block Chaining.", Advances in Cryptology-CRYPTO '94, pp. 341-358
	A7	Federal Information Processing Standards Publication 46-1, Data Encryption Standard (DES), pp. 1-16, (1988)
	A8	Federal Information Processing Standards Publication 46-2, Data Encryption Standard (DES), pp. 1-18, (1993)
	A9	Erez PETRANK et al., "CBC MAC For Real-Time Data Sources", Federal Information Processing Standards Publication 46-2, Data Encryption, pp. 1-23, (1993)
	A10	American National Standard ANSI X9.9 (1986) pp. 6-8
	A11	Mihir BELLARE et al., "XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions", pp. 1-20, (1995) Preliminary version appearing in Advances in Cryptology-CRYPTO '95, Lecture Notes in Computer Science vol. 963.
	A12	Mihir BELLARE et al., "Incremental Cryptography and Application to Virus Protection.", pp. 1-15, (1995), Abstract appearing in Proceedings of the 27th ACM Symposium on the Theory of Computing, May (1995)
	A13	Moni NAOR et al., "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs.", Advances In Cryptology-CRYPTO '98, Springer-Verlag Berlin Heidelberg, pp. 265-282, (1998)
	A14	Mihir BELLARE et al., "A Concrete Security Treatment of Symmetric Encryption", Proceedings of the 38th Sympposium on Foundations of Computer Science, IEEE,(1997) pp. 394-403
	A15	Donald E. KNUTH., "The Art of Computer Programming-Vol. 2: Seminumerical Algorighms.", Addison-Wesley, (1981) (Second Edition), Chapter 3.

EXAMINER	DATE CONSIDERED
[signature]	6/9/05

* **EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.**

Form PTO-1449 (MODIFIED)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. 068398-0104	SERIAL NO. 09/818,608
INFORMATION DISCLOSURE CITATION		APPLICANT Virgil D. Gligor et al.	
(Use several sheets if necessary)		FILING DATE 03/28/2001	GROUP ART UNIT Unassigned

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

MDN	A1	GLIGOR et al., "Object Migration And Authentication", *IEEE Transactions On Software Engineering*, Vol. SE-5(6):607-611, (1979) *
MDN	A2	MENEZES et al., ""Handbook of Applied Cryptography", pp. 321-367, (1965) *
	A3	GILBERT et al., "A Chosen Plaintext Attack Of The 16-Round Khufu Cryptosystem", pp. 340-358, (1988)
	A4	DESMEDT, "Advances In cryptology – CRYPTO '94", 14th Annual International Cryptology Conference, pp. 1-19, (1994) *
	A5	BELLARE et al., "Keying Hash Functions For Message Authentication", Springer-Verlag Berlin Heidelberg, pp. 216-233, (1996)
	A6	WIENER, "Advances In Cryptoloty – CRYPTO '99", 19th Annual International Cryptology Conference, pp. 368-383, (1999) *
	A7	Federal Information Processing Standards Publication 46-2, Data Encryptioin Standard (DES), pp. 1-5, (1993)
	A8	PETRANK et al., "CBC MAC For Real-Time Data Sources", Federal Information Processing Standards Publication 46-2, Data Encryptioin, pp. 1-18 and 1-23, (1993)
	A9	BELLARE et al., "XOR MACs: new Methods for Message Authentication Using Finite Pseudorandom Functions", pp.1-20 and 1-15, (1995) *
	A10	KRAWCZYK, "Advances In Cryptology CRYPTO '98", Springer-Verlag Berlin Heidelberg,pp.265-282, (1998) *
	A11	BELLARE et al., "A Concrete Security Treatment of Symmetric Encryption", pp. 394-404, (1996)

EXAMINER	DATE CONSIDERED
[signature]	6/9/05

* **EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.**